Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Tuesday, October 24, 2006

Things as authorities

When we hear the word "authority" we often think of people who have set themselves up in positions of power and on whom we have become dependent. But there is another kind of authority, often more reliable and trustworthy, that can be provided by things. These are physical standards, security devices, automata, and other objects by which we coordinate our interactions with fellow humans, especially with strangers who might not otherwise be trustworthy. These technologies are crucial to our modern civilization and its ability to make dealings with strangers more secure and reliable.

Authoritative automata often come in the form of what (on a computer) Mark Miller has dubbed an admonition system. An admonition system reminds a person of a plan or of a legal or ethical obligation. A clock, for example, can remind a person of a scheduled meeting, and a cash register communicates an obligation to pay.

With some extra security a device may also provide a strong affordance that requires the person to act purposefully to use it or to avoid using it, and may also gather evidence of such use or avoidance, as with tamper evidence. A locked door, for example, reminds a person about whether they have consent to enter, makes accidental entry effectively impossible, and often requires those who enter anyway to leave behind evidence of lock picking or forcible entry.

Some technologies create standards that we all come to follow, as in standard weights and measures. Old unforgeably costly standards, such as those of shells used in hunter-gatherer and Neolithic cultures and the gold standard used up to modern times, enabled the emergence of money to replace barter and other costly and inconvenient in-kind

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

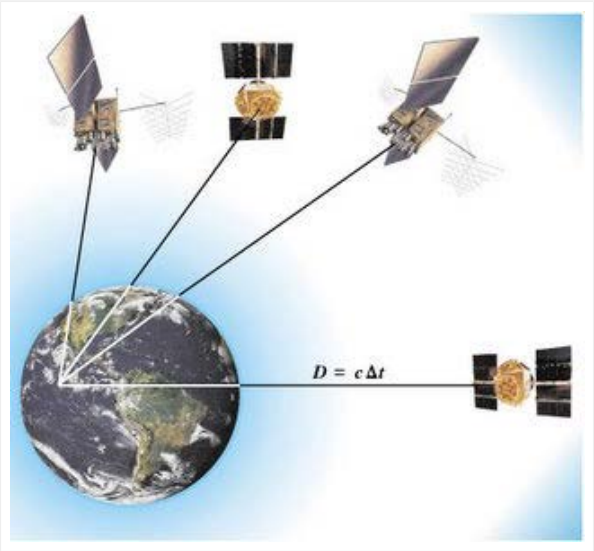
View my complete profile

transactions. Physical standards provide objective, verifiable, and repeatable interactions with our physical environment and with each other.

When new kinds of authoritative automata are proposed, the robotic response of Hello Kitty people is that they are inflexible and impersonal and thus not to be trusted. The Roman playwright Plautus made fun of early complainer of this kind, a bum objecting to one of the earliest authoritative devices, the sundial:

> The gods confound the man who first found out
> How to distinguish the hours. Confound him too,
> Who in this place set up a sundial,
> To cut and hack my days so wretchedly
> Into small pieces! When I was a boy,
> My belly was my sundial -- only surer,
> Truer, and more exact than any of them.
> This dial told me when 'twas the proper time
> To go to dinner, when I ought to eat;
> But nowadays, why even when I have,
> I can't fall to unless the sun gives leave.
> The town's so full of these confounded dials!

But history teaches that it is the many people who act strategically against strangers who are not to be trusted. It is human preferences, not machines, that are unpredictable and incomparable, as well they should be. For coordinating our interactions with strangers, impartial automata are often crucial.



To what extent will computer algorithms come to serve as authorities? We've already seen one algorithm that has been in use for centuries: the adding algorithm in adding machines and cash registers. Some other authoritative algorithms have become crucial parts of the following:

(1) All the various protocols network applications use to talk to each other, such the web browser protocol you are probably using right now,

(2) The system that distributes domain names (the name of a web site found in an URL) and translate them to Internet protocol (IP) addresses -- albeit, not the ability to register domain names in the first place, which is still largely manual,

(3) Ranking algorithms such as Google page rank (for relevance based on a particular text search) and popularity ranking algorithms such as those used

Blog Archive

► 2018 (1)
► 2017 (3)
► 2016 (4)
► 2015 (3)
► 2014 (3)
► 2013 (3)
► 2012 (8)
► 2011 (12)
► 2010 (9)
► 2009 (29)
► 2008 (55)
► 2007 (47)
▼ 2006 (130)
► December (4)
► November (7)
▼ October (15)
Things as authorities
Fifty years ago today
The pigeonhole principle
Three kinds of jurisdiction
Citron's "data reservoirs": putting liability at t...
How to succeed or fail on a frontier
600,000 excess deaths in Iraq since U.S. invasion
Visual mathematics
Prosecute U.S. Justice Department lawyers as war c...
Hungarian Revolution anniversary
Liberty and habeas corpus (II)
New fun legal specialty
The Lex Gabina: ancient

by Digg, Reddit, and the like,

(4) Payment systems, such as credit card processing and PayPal,

(5) Time distribution networks and protocols,

(6) The Global Positioning System (GPS) for determining location based on the time it takes radio signals to travel from a orbiting satellites, and

(7) A wide variety of other algorithms that many of us rely on to coordinate our activities.

Algorithms give us the potential of moving beyond the weak and reactive security of most physical devices to strong and often preventative security. Technologies such as digital signatures and mulitparty private computation may be used to implement things like unalterable audit trails, smart contracts, secure and owner-controlled property title registries, and so on. Bit gold, or property titles to unforgeably costly bits, might be possible. These automata will rely more on distribution and protocol security and less on trusted third parties than traditional authorities. There is a strong argument to be made that algorithmic authorities should be open source.

We've just scratched the surface of what secure authorities we can establish over computer networks. Such authorities will make it far easier for 6 billion plus strangers to interact with each other securely and reliably.

Posted by Nick Szabo at 9:25 PM

Military Commissions Act?
Hello Kitty people
Liberty and habeas corpus (I)
► September (15)
► August (20)
► July (5)
► June (10)
► May (4)
► April (3)
► March (11)
► February (10)
► January (26)
► 2005 (44)

7 comments:

Jeremy said...

Enjoyed your post, just have a few reactions.

In an earlier post's comments you worried about private gaming of an authoritive automaton. Another problem I have with this

"systems ueber alles" mindset is that besides being subject to manipulation it also encourages centralization of authority. In some cases setting one rule by which everybody plays may be desirable, but not in all.

I'm also concerned with the State's role in subsidizing the costs of what would otherwise be untenable authoritative automata such the money supply, financial networks, and other heavily regulated/cartelized systems. The State promotes "stability" to the exclusion of a lot of basic individualist interests far too often, and the kind of disinterested automata you speak of seem right along those lines. When the systems start to substitute coercive implementation of central authority for what is otherwise simple reinforcement of social norms, it is clear to me that we may not have an efficient system here.

Human beings can be very skeptical of what they see as excessive or needless complexity. Law is a great example of how what is really a pretty simple concept has been "systematized" outside the grasp of any person of average intelligence. Gaming of this system is practically a given. Centralized systems are fine when the costs outweigh the benefits, but with the distorting effects of State intervention, it is often hard to tell exactly which way the scale tips.

10:01 AM

Nick Szabo said...

Jeremy, I share your concerns, and those concerns are just why I'm so enthusiastic about authority from things. In its ideal form the authoritative object cannot be manipulated by any human or group of humans, no matter how powerful. To the extent we can approach this ideal we reduce our vulnerabilities to gaming and centralization of authority.

As something that comes quite close to this ideal, think of a pulsar as a time standard. A pulsar sits far beyond the distance where it can be subject to any human manipulation, sending out a precisely regular strobe. As long as you control a machine that picks up this signal directly, nobody else can defraud you as to what time it is.

With current technology it's too expensive for the vast majority of people, including me, to pick up a pulsar radio signal with our own receivers. So I have to rely on some other people to pick up the signal (or, as it really works today, measure the signal of atomic clocks of the same kind) and tell me what time it is: I have to rely on some communications and some trust, or at least on some security beyond my control. If I talk directly to the people who do have such radio receivers, then if at least one over a half of these people are reliable a minority of colluding liars can't defraud me. I can tell something untoward is going on in a debugged system even with a small number of errors, but if fewer than half are defrauding me, I still know what the time is. The more uncontrolled and independent people I talk to the more restitant I am to manipulation or fraud by a powerful person or group.

In practice, because time can ultimately be measured against astronomical objects beyond reach, and proximately based on regular mechanical or standard atomic movements, it has long been difficult for central authorities to defraud people in most ways about the time. There are stories that employers once used to add few minutes to every hour back when they controlled the only clock in the factory, but if so this became impossible when at least a few employees started carrying pocket watches.

It's an interesting question as to whether the U.S. government ever has or could undetectably defraud GPS users. Fortunately the EU is launching an alternative called Galileo which will make this even less likely.

Traditionally we have come up with many processes to greatly improve the reliability of communications: tamper-evidence (as in sealed letters), physical broadcast (where it's hard to prevent people from receiving accurately what was broadcast), hard-to-forge audit trails, separation of duties, scientific methods of repeating experiments, and so on.

The cryptographic research community studies protocols with very strong mathematical properties, such that (most likely) one would have to expend vast amounts of energy, often even more energy than is available in the entire universe, to break the protocol. Encryption, digital signatures, mulitparty secure computation, and a variety of other useful protocols probably have such strong properties.

Real implementations, alas, don't quite live up to this ideal and are sometimes cracked. But overall cryptography can provide a great leap up in the security of a variety of communications, such as the unalterability of audit trails. Thus I foresee a future in which

automata as authority will become far more reliable and secure and will replace many weaker traditional methods. As a result we'll have a much more secure basis on which to trust our six billion plus fellow strangers with much less reliance than in the past on central authorities.

10:34 PM

Jeremy said...

Thanks for your response.

I totally agree with your point about a disinterested automaton like a pulsar star for time. To me, the key is not the accuracy of the automaton, but the variety of possible authorities available, so that competition can occur. This requires people to be knowledgeable, however, about the nature of the authority behind the system - something many find tedious.

Right now I'm reading "Secrets of the Temple", the seminal work on the Federal Reserve. One of the key points in the book was the movement among the board members to follow a single measure of the growth of the money supply (M1) and peg all their actions to it, so that they could claim to act in a disinterested, mechanistic manner (of course, the idea that the money supply is not influenced by the Fed is patently ridiculous). Of course, disaster eventually ensued and nobody was happy in the end, but moreover - the Fed found ways to do what it wanted and make it LOOK like they were adhering to the automaton's authority.

Of course, the Fed is a monopoly, which is why I think your point about open source is so important: let the market determine which authority is most authoritive.

8:28 AM

Rick OBrien said...

Without code review, how else can one know for certain whether or not the Voice UI / algorithms in Amazon's Echo-Alexa are red-lining comparative search results or skewing prices according to one's payment history? Do we need an Underwriter's Lab service for cyber that issues credentials after testing algorithmic expressions conform to human friendly specifications that adhere to principles defined in Model Law?

4:44 PM

Nick Gogerty said...

any thoughts on self sovreign and federated identities which may emerge as networks of decentralized authorities? Seems like an exciting concept, localized bounded truth for small problems.

9:41 PM

Anonymous said...

Thanks Nick for another thoughtful and thought provoking post. It took me a couple of reads to put it in focus. I was bothered by the word authority (somehow I always am), but it boils down to semantics. Authority could be associated with enforcement or simply with communication. You are an authority on digital money, in the sense that your superior knowledge, when communicated, can be relied upon by others, not in the sense that you can decide and enforce decisions on digital money.
So is the North Star, or the Eastern Seaboard Fission Authority, whose familiar shape allowed Neuromancers' characters to recognize the neighborhood. The Berlin Wall, or minefields in the DMZ, on the other hand, were a different kind of authority, because they physically prevented comrades from, and sanctioned them for, crossing through.
This distinction is, I think, particularly important in the digital realm, since there you can have authorities that are more like the wall. It is not the same to have an authority that says 'ding dong, it's time to pay interest' as one that says 'ding dong, I have just paid interest since it is due according to the contract'.

The power of the latter, in the context of consensuality, is even more awesome, as it has been shown since you wrote this post.

7:04 AM

elzr said...

Loved this post, you had me at the title :) Traffic lights are mentioned as a photo but I'll just add that I'm endlessly fascinated with this crucial piece of our current global infrastructure: a very simple artifact (in essence just a color code, lights & clock) can coordinate multitudes of competing persons, doing it better & infinitely more scalably than a cuddly person could (imagine traffic cops at EVERY intersection).

Joseph Heath, in his classic *The Efficient Society*, uses the traffic light metaphorically to illustrate a key distinction about efficiency:

"Society does not exist in order to produce any one thing, and so it cannot do so efficiently or inefficiently. Our society is efficient because it enables us, its members, to act efficiently. It *facilitates* efficiency. It allows us to go about our business with a minimum of hassle. **It is more like a trafiic light than a steam engine.**"

Hello Kitty people is an interesting name for that widespread, naive fetish for cuddly humans in fuzzy arrangements instead of artifacts & clear processes (a far more common fetish among the lefts, I daresay, even the modern ones, so enamoured with face-to-face, "direct" participation).

Have you read Bruno Latour's 1992 essay *Where are the Missing Masses?* http://www.bruno-latour.fr/sites/default/files/50-MISSING-MASSES-GB.pdf In about 30 delightful & brilliant pages he makes a very related thesis to yours: non-humans (artifacts) are the unaccounted masses of morality/authority in society.

(I wrote this comment since December 25, 2016 but it wasn't published. Trying again in case its disaproval was a mistake. Thanks!)

8:19 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.